

REMARKS

Claims 111-116 are copied substantially verbatim from U.S. Patent Application No. 09/948,806, Publication No. 2002/0048369, published April 25, 2002, for Ginter et al. (hereinafter "Ginter Appl. '806"). Added claims 111, 112, 113, 114, 115, and 116 correspond to Ginter Appl. '806 claims 1, 2, 3, 4, 7, and 8, respectively.

Claims 117-144 are copied substantially verbatim from U.S. Patent Application No. 09/764,370, Publication No. 2002/0112171, published August 15, 2002, for Ginter et al. (hereinafter "Ginter Appl. '370"). Added claims 117-144 correspond to Ginter Appl. '370 claims 1, 13-16, 36-37, 45, 49, 55, 58, 60, 64-67, 70-76, 79-81, and 89-90. A one-to-one correspondence between the added claims and the Ginter Appl. '370 claims is shown in Table 1 below.

Added Claim No.	Ginter Appl. '370 Claim No.
117	1
118	13
119	14
120	15
121	16
122	36
123	37
124	45
125	49
126	55
127	58
128	60
129	64
130	65
131	66
132	67
133	70
134	71
135	72
136	73
137	74
138	75
139	76
140	79
141	80
142	81
143	89
144	90

Table 1

In accordance with 37 C.F.R. § 1.604, the copied claims may be specifically applied to Applicants' disclosure as follows:

<p align="center">Copied Claim From InterTrust Published Patent Application (Ginter et al., Pub. No. US 2002/0048369 A1)</p>	<p align="center">Applicants' Disclosure In Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)</p>
<p>111. A rights management appliance including:</p>	<p>Applicants disclose a data processor (i.e., an appliance) to be used for managing data objects (i.e., for rights management). (p.8, l.25-p.9, l.9; p.17, ll.1-12).</p>
<p>a user input device,</p>	<p>Applicants disclose a keyboard (i.e., a user input device). (p.9, l.1; FIG.2).</p>
<p>a user display device,</p>	<p>Applicants disclose a display (i.e., a user display device). (p.9, l.1; FIG.2).</p>
<p>at least one processor, and</p>	<p>Applicants disclose a data processor including a CPU (i.e., a processor). (p.8, ll.29-30).</p>
<p>at least one element defining a protected processing environment,</p>	<ul style="list-style-type: none"> • Applicants disclose a user program including a decryption module and one or more security modules (i.e., at least one element) operably coupled to a user's data processor. (p.17, ll.15-20). If the proper format and security modules are not available for a particular data object, usage is not permitted (i.e., a protected processing environment). (p.18, ll.3-5). • The user program can have code which controls use of the program by password. (p.18, ll.13-14). • The data object is never stored in native format in user accessible storage. (p.18, ll.22-24). • Applicants disclose that the data provider's data processor is considered secure. (p.9, ll.8-9).

characterized in that the protected processing environment stores and uses permissions, methods, keys, programs and/or other information to electronically manage rights.

Applicants disclose that a user/data provider's data processor utilizes control data, security modules including keys, decryption modules, and programs (i.e., permissions, methods, keys, programs, and/or other information) to control the usage of a data object (i.e., electronically manages rights). (p.17, ll.15-20; p.21, l.17-p.22, l.12)

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0048369 A1)</p>	<p>Applicants' Disclosure In Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
112. In a rights management appliance including:	<i>See Claim 111 above.</i>
a user input device,	<i>See Claim 111 above.</i>
a user display device,	<i>See Claim 111 above.</i>
at least one processor, and	<i>See Claim 111 above.</i>
at least one element defining a protected processing environment,	<i>See Claim 111 above.</i>
a method of operating the appliance characterized by the step of storing and using permissions, methods, keys, programs and/or other information to electronically manage rights.	<i>See Claim 111 above.</i>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0048369 A1)</p>	<p>Applicants' Disclosure In Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>113. A rights management appliance including at least one processor element at least in part defining a protected processing environment, characterized in that the protected processing environment stores and uses permissions, methods, keys, programs and/or other information to electronically manage rights.</p>	<p><i>See Claim 111 above.</i></p>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0048369 A1)</p>	<p>Applicants' Disclosure In Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>114. In a rights management appliance including at least one processor element at least in part defining a protected processing environment, a method comprising storing and using permissions, methods, keys, programs and/or other information to electronically manage rights.</p>	<p><i>See Claim 111 above.</i></p>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0048369 A1)</p>	<p>Applicants' Disclosure In Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>115. An electronic appliance arrangement containing a protected processing environment and at least one secure database operatively connected to said protected processing environment, said arrangement including means to monitor usage of at least one aspect of an amount of appliance usage and control said usage based at least in part upon protected appliance usage control information processed at least in part through use of said protected processing environment.</p>	<ul style="list-style-type: none"> • See Claim 111 above. • Applicants disclose at least a database 20 for control data. (p.9, ll.6-7). • Applicants further disclose that a security module may implement an authorization process, according to which each usage of the data object requires a dial up to the data processor of the data object provider. (p.22, ll.1-12; p.23, l.29-p.24, l.2). • Applicants disclose the “control data structure can include control elements for complex user types, usage types . . .” (i.e., appliance usage). “Security modules could require a dial up to the brokers data processor to approve loading or usage actions . . .” (p.25, ll.8-13).

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0048369 A1)</p>	<p>Applicants' Disclosure In Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>116. In an electronic appliance arrangement containing a protected processing environment and at least one secure database operatively connected to said protected processing environment, a method characterized by the steps of monitoring usage of at least one aspect of appliance usage and controlling said usage based at least in part upon protected appliance usage control information processed at least in part through use of said protected processing environment.</p>	<p><i>See Claim 115 above.</i></p>

<p align="center">Copied Claim From InterTrust Published Patent Application</p> <p align="center">(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p align="center">Applicants' Disclosure in Appl. No. 09/321,386</p> <p align="center">(MDNA1.C2.US) (M-15081US)</p>
<p>117. A secure component-based operating process including:</p>	<p>Applicants disclose the handling of composite data objects (e.g., software) (i.e., component-based processes). (p.24, l.11-p.25, l.3).</p>
<p>(a) retrieving at least one component;</p>	<ul style="list-style-type: none"> • Applicants disclose the use or formation of composite objects comprising constituent objects (i.e., one component). (p.24, ll.12-14). • Furthermore, Applicants disclose buy and sell order packages (i.e., at least one component) are received by a stock trading data processor (pp.26-27).
<p>(b) retrieving a record that specifies a component assembly;</p>	<ul style="list-style-type: none"> • Applicants disclose utilizing a control data format with control elements defining relationships between constituent objects and defining a parent/child element (i.e., a record that specifies component assembly). (p.24, ll.12-14). • Furthermore, Applicants disclose the buy and sell order packages each include control data for a match (i.e., a record that specifies component assembly).

<p>(c) checking said component and/or said record for validity;</p>	<ul style="list-style-type: none"> • Applicants disclose that a general set of control data comprises a security control element which defines a security procedure which has to be carried out before usage of a data object. (p.4, ll.17-19). • The “security” disclosed by Applicants relates generally to “encryption” methods and “authorization” algorithms (e.g., RSA and key methods) (i.e., checking said component and/or said record for validity). (p.21, ll.17-31).
<p>(d) using said component to form said component assembly in accordance with said record; and</p>	<ul style="list-style-type: none"> • Applicants disclose combining data objects to create a new data object created with control data linking the constituent data objects (i.e., using said component to form said component assembly). (p.24, ll.27-30). • Applicants disclose a broker who can include a video (i.e., a component) and text book (i.e., a component) in an educational package (i.e., assembly). (p.24, ll.11-31). • Furthermore, Applicants disclose a match between the buy and sell order packages results in a transfer of digital money with repackaged and updated data packages (i.e., component assembly). (p.26, l.29-p.27, l.2).

<p>(e) performing a process based at least in part on said component assembly.</p>	<ul style="list-style-type: none"> • Applicants disclose that a general set of control data is created for a composite data object that can be distributed by a broker to a user. (p.24, ll.11-31). • Applicants disclose enabling data object usage and limiting the number of usages based upon control data (i.e., performing a process based at least in part on said component assembly). (p.19, ll.26-30). • Furthermore, Applicants disclose the new data packages after a match are transferred back to the seller and buyer data processors (i.e., performing a process). (pp.26-27)
--	--

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
118. A secure component operating system process including:	<i>See Claim 117 above.</i>
receiving a component;	<i>See Claim 117(a) above.</i>
receiving directions specifying use of said component to form a component assembly;	<i>See Claim 117(b) above.</i>
authenticating said received component and/or said directions;	<i>See Claim 117(c) above.</i>
forming, using said component, said component assembly based at least in part on said received directions; and	<i>See Claim 117(d) above.</i>
using said component assembly to perform at least one operation.	<i>See Claim 117(e) above.</i>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>119. A method comprising performing the following steps within a secure operating system environment:</p>	<p>Applicants disclose that the user's data processor is a secure processor (p.9, ll.8-9) requiring certain security modules for usage of the data object (i.e., a secure operating system environment. (p.18, ll.3-5).</p>
<p>providing code;</p>	<p>Applicants disclose providing of a data object, which can include software (i.e., code). (p.2, l.3).</p>
<p>providing directions specifying assembly of said code into an executable program;</p>	<p>See Claim 117(b) above.</p>
<p>checking said received code and/or said assembly directions for validity; and</p>	<p>See Claim 117(c) above.</p>
<p>in response to occurrence of an event, assembling said code in accordance with said received assembly directions to form an assembly for execution.</p>	<ul style="list-style-type: none"> Applicants disclose that in response to an authorization to use (i.e., an event), a user may access a data object. (p.5, ll.25-30; p.19, ll.20-25). A data object may include composite data objects. Constituent data objects may be combined to create a composite data object (i.e., an assembly) for some particular use, created with control data linking the constituent data objects (i.e., assembling said code in accordance with received assembly instructions). (p.24, ll.27-30).

<p align="center">Copied Claim From InterTrust Published Patent Application</p> <p align="center">(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p align="center">Applicants' Disclosure in Appl. No. 09/321,386</p> <p align="center">(MDNA1.C2.US) (M-15081US)</p>
<p>120. A method for managing at least one resource with a secure operating environment, said method comprising:</p>	<ul style="list-style-type: none"> • Applicants disclose management of data objects for distribution by an author, broker, or user (i.e., a resource). (p.1, ll.14-16; p.8, ll.26-29; p.14, ll.25-30). • Applicants disclose a secure operating environment. <i>See</i> Claim 119 above.
<p>securely receiving a first control from a first entity external to said operating environment;</p>	<ul style="list-style-type: none"> • Applicants disclose usage conditions with a data object (i.e., a first control) from an author (i.e., a first entity) may be sent to a broker's data processor (i.e., operating environment). (p.8, ll.9-17). • Applicants disclose buy and sell order with control data are received by a stock trading data processor. (pp.26-27).
<p>securely receiving a second control from a second entity external to said operating environment, said second entity being different from said first entity;</p>	<ul style="list-style-type: none"> • Applicants disclose a broker may repackage a received data object and add further control data (i.e., a second control) which is relevant to his business activities. (p.8, ll.9-17). • Applicants further disclose a broker may combine constituent data objects into a composite data object for distribution. (p.24, ll.11-24). • Thus, it is at least inherent that a second data object with a second set of control data from a different author than the first could be sent to a broker's data processor. • Applicants disclose the buy and sell control data are sent from two different entities. (pp.26-27).

securely processing, using at least one resource, a data item associated with said first and second controls; and	<ul style="list-style-type: none"> • Applicants disclose a broker including a video data object and a text book data object in an educational package (i.e., a data item). (p.24, ll.12-19). • See Claim 117(e) above. • Applicants further disclose that the buy and sell order control data are used in conjunction to transfer digital money (i.e., a data item). (pp.26-27).
securely applying said first and second controls to manage said resource for use with said data item.	Applicants disclose a broker adding program procedures to program modules to process the control elements of constituent objects. (p.24, ll.12-19).

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>121. A method for securely managing at least one operation on a data item performed at least in part by an electronic arrangement, said method comprising:</p>	<p>Applicants disclose management of data objects (i.e., data items) for distribution by a broker, agent, or user (i.e., by an electronic arrangement – agreements between participants in a commercial value chain and/or a data security chain model for handling, auditing, reporting, and payment). (p.1, ll.14-16; p.8, ll.26-29; p.14, ll.25-30).</p>
<p>(a) securely delivering a first procedure to said electronic arrangement;</p>	<p>Applicants disclose usage conditions (i.e., a first procedure) from an author may be sent to a broker's data processor with a data object. (p.8, ll.9-17).</p>

(b) securely delivering, to said electronic arrangement, a second procedure separable or separate from said first procedure;

- Applicants disclose a broker may repackage a received data object and add further control data (i.e., a second procedure) which is relevant to his business activities. (p.8, ll.9-17).
- Applicants further disclose a broker may combine constituent data objects with constituent control data into a composite data object for distribution. Each constituent data object retains its original control data which continues to control its subsequent usage. (p.24, ll.11-31).
- Thus, it is at least inherent that a second data object with a second set of control data (i.e., a second procedure) may be delivered to a broker's data processor.
- Furthermore, Applicants disclose that a user requests authorization (i.e., a second procedure) to use a data object. (p.5, ll.25-30; p.19, ll.8-12).
- Applicants further disclose two different sets of control data (buy and sell orders) are sent to a stock trading data processor. (pp.26-27).

<p>(c) performing at least one operation on said data item, including using said first and second procedures in combination to at least in part securely manage said operation; and</p>	<ul style="list-style-type: none"> • Applicants disclose enabling data object usage and limiting the number of usages based upon control data. (p.19, ll.26-30). • Applicants further disclose that a usage manager module compares the user request for usage with the corresponding control data (i.e., using said first and second procedures in combination). If the requested usage is not permitted in the control data, the requested usage is disabled. (p.19, ll.20-25). • See Claims 117(e) and 120 above. • Applicants further disclose that the buy and sell order control data are used in conjunction to transfer digital money (i.e., a data item). (pp.26-27).
<p>(d) securely conditioning at least one aspect of use of said data item based on said delivering steps (a) and (b) having occurred.</p>	<ul style="list-style-type: none"> • It is inherent that if a user does not request usage, no use of the data object will occur. • Applicants also disclose an automated transaction negotiation in which digital money is not transferred without a matching of a delivered sell order and a delivered buy order. (pp.26-27).

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>122. A method for securely managing at least one operation performed at least in part by a secure electronic appliance, comprising:</p>	<p>Applicants disclose management of data objects using data processors including security modules (i.e., a secure electronic appliance). (p.8, 1.25-p.9, 1.9).</p>
<p>(a) selecting an item that is protected with respect to at least one operation;</p>	<p>See Claim 121(c) above.</p>
<p>(b) securely independently delivering plural separate procedures to said electronic appliance;</p>	<p>See Claim 121(a) and 121(b) above.</p>
<p>(c) using said plural separate procedures in combination to at least in part securely manage said operation with respect to said selected item; and</p>	<p>See Claims 117(e) and 121(c) above.</p>
<p>(d) conditioning successful completion of said operation on said delivering step (b) having occurred.</p>	<p>See Claim 121(d) above.</p>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
123. A method for processing based on independent deliverables comprising:	<i>See Claim 117 above.</i>
securely delivering a first piece of code defining a first part of a process;	<i>See Claims 120 and 121(a) above.</i>
separately, securely delivering a second piece of code defining a second part of said process;	<i>See Claims 120 and 121(b) above.</i>
ensuring the integrity of the first and second delivered pieces of code; and	<i>See Claim 117(c) above.</i>
performing said process based at least in part on said first and second delivered code pieces.	<i>See Claims 117(e) and 120 above.</i>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>124. A method of securely controlling at least one protected operation with respect to a data item comprising:</p>	<p><i>See Claim 121(c) above.</i></p>
<p>(a) supplying at least a first control from a first party;</p>	<p><i>See Claims 120 and 121(a) above.</i></p>
<p>(b) supplying at least a second control from a second party different from said first party;</p>	<p><i>See Claims 120 and 121(b) above.</i></p>
<p>(c) securely combining said first and second controls to form a set of controls;</p>	<p><i>See Claims 117(d), 117(e), and 120 above.</i></p>
<p>(d) securely associating said control set with said data item; and</p>	<p><i>See Claim 117(d) and 117(e) above.</i></p>
<p>(e) securely controlling at least one protected operation with respect to said data item based on said control set.</p>	<p><i>See Claims 120 and 121(c) above.</i></p>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>125. A secure method for combining data items into a composite data item comprising:</p>	<p>Applicants disclose the handling of composite data objects including constituent data objects. (p.24, ll.11-24).</p>
<p>(a) securely providing a first data item having at least a first control associated therewith;</p>	<p><i>See Claims 117(a), 120, and 121(a) above.</i></p>
<p>(b) securely providing a second data item having at least a second control associated therewith;</p>	<p><i>See Claims 120 and 121(b) above.</i></p>
<p>(c) forming a composite of said first and second data items;</p>	<p><i>See Claim 117(d) above.</i></p>
<p>(d) securely combining said first and second controls into a composite control set; and</p>	<p><i>See Claim 117(e) above.</i></p>
<p>(e) performing at least one operation on said composite of said first and second data items based at least in part on said composite control set.</p>	<p><i>See Claim 117(e) above.</i></p>

<p align="center">Copied Claim From InterTrust Published Patent Application</p> <p align="center">(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p align="center">Applicants' Disclosure in MDNA1.C2.US</p> <p align="center">(M-15081US)</p>
126. A secure method for controlling a protected operation comprising:	<i>See Claim 121 above.</i>
(a) delivering at least a first control and a second control; and	<i>See Claims 120, 121(a), and 121(b) above.</i>
(b) controlling at least one protected operation based at least in part on a combination of said first and second controls, including at least one of the following steps:	<i>See Claim 121(c) above.</i>
resolving at least one conflict between said first and second controls based on a predefined order,	<ul style="list-style-type: none"> • Applicants disclose matching and non-matching between two sets of buy and sell control data (i.e., resolving conflict based on a predefined order). (pp.26-27). • Applicants disclose a composite object can be handled by defining a control data format with control elements defining relationships between constituent objects and by defining a parent/child element. (p.24, ll.12-14). • It is also at least inherent in the formation of composite objects that conflicts between the control data of the constituent objects will be resolved based on a predefined order.
providing an interaction with a user to form said combination; and	Applicants disclose a user can combine data objects for some particular purpose. (p.24, ll.27-31). <i>See also</i> Claim 117(d) above.
dynamically negotiating between said first and second controls.	Applicants disclose an automated transaction negotiation method between two sets of control data. (pp.26-27).

<p align="center">Copied Claim From InterTrust Published Patent Application</p> <p align="center">(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p align="center">Applicants' Disclosure in Appl. No. 09/321,386</p> <p align="center">(MDNA1.C2.US) (M-15081US)</p>
<p>127. A secure method comprising:</p>	<p>Applicants disclose a secure method.</p>
<p>selecting protected data;</p>	<ul style="list-style-type: none"> • Applicants disclose data objects protected in a package. (p.9, ll.12-14). • Furthermore, Applicants disclose digital money (i.e., protected data) in a buy and sell negotiation. (pp.26-27).
<p>extracting said protected data from an object;</p>	<ul style="list-style-type: none"> • Applicants disclose a user extracting protected data from a data package. (p.19, ll.20-28). • Furthermore, Applicants disclose that the user program executes a transaction whereby the digital money (i.e., protected data) is extracted from the buy order data package and transferred to the sell order package. (p.26, l.29-p.27, l.2).
<p>identifying at least one control to manage at least one aspect of use of said extracted data;</p>	<ul style="list-style-type: none"> • Applicants disclose control data associated with a constituent data object and control data associated with a composite data object. (p.24, ll.20-31; FIG. 17). • Furthermore, Applicants disclose the control data of the sell order data package (i.e., at least one control) is updated after the matching of buy and sell orders and transfer of digital money (i.e., extracted data). (pp.26-27).

<p>placing said extracted data into a further object; and</p>	<ul style="list-style-type: none"> • Applicants disclose creating a parent object with constituent objects and combining data objects. (p.24, ll.12-31). • Furthermore, Applicants disclose transfer of digital money to the sell order package (i.e., a further object). (pp.26-27).
<p>associating said at least one control with said further object.</p>	<ul style="list-style-type: none"> • Applicants disclose control data associated with a constituent data object and control data associated with a composite data object. (p.24, ll.20-31; FIG. 17). • Control elements may define relationships between constituent objects and a parent/child relationship. (p.24, ll.12-14). • Furthermore, Applicants disclose the control data of the sell order data package (i.e., at least one control) is updated after the matching of buy and sell orders and transfer of digital money (i.e., extracted data). (pp.26-27).

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>128. A secure method of modifying a protected object comprising:</p>	<p>Applicants disclose combining data objects to create a new data object (i.e., a protected object is modified). (p.24, ll.27-31).</p>
<p>(a) providing a protected object; and</p>	<p>Applicants disclose protected data objects.</p>
<p>(b) embedding at least one additional element into said protected object without unprotecting said object.</p>	<p>Applicants disclose combining data objects to form a new data object (i.e., embedding an element into the protected object) with control data linking the constituent data objects. Each constituent data object retains its original control data which continues to control its subsequent usage. (p.24, ll.12-31).</p>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>129. A method for managing at least one resource with a secure operating environment, said method comprising:</p>	<p><i>See Claim 120 above.</i></p>
<p>securely receiving a first load module from a first entity external to said operating environment;</p>	<ul style="list-style-type: none"> • <i>See Claim 120 above.</i> • A "load module" is equivalent to a "control".
<p>securely receiving a second load module from a second entity external to said operating environment, said second entity being different from said first entity;</p>	<ul style="list-style-type: none"> • <i>See Claim 120 above.</i> • A "load module" is equivalent to a "control".
<p>securely processing, using at least one resource, a data item associated with said first and second load modules; and</p>	<ul style="list-style-type: none"> • <i>See Claim 120 above.</i> • A "load module" is equivalent to a "control".
<p>securely applying said first and second load modules to manage said resource for use with said data item.</p>	<ul style="list-style-type: none"> • <i>See Claim 120 above.</i> • A "load module" is equivalent to a "control".

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>130. A method for negotiating electronic contracts, comprising:</p>	<p>Applicants disclose an automated transaction negotiation. (pp.26-27).</p>
<p>receiving a first control set from a remote site;</p>	<p>Applicants disclose a seller/buyer that creates control data, e.g. kind of stock, price, quantity (i.e., a first control set) on the seller's/buyer's data processor (i.e., a remote site) to participate in a negotiation. The rules or conditions for buying and selling stocks are indicated in the control data. (p.26).</p>
<p>providing a second control set;</p>	<p>Applicants disclose a buyer's/seller's control data (i.e., a second control set).</p>
<p>performing, within a protected processing environment, an electronic negotiation between said first control set and said second control set, including providing interaction between said first and second control sets; and</p>	<ul style="list-style-type: none"> • Applicants disclose performing automated negotiations at the data processor of the stock trading company (i.e., a protected processing environment). (p.27, ll.3-4). • Applicants disclose that the control data of the sell (i.e., first control set) and buy (i.e., second control set) order packages are examined and matched (i.e., providing interaction between said first and second control sets) by the user program of the stock trading company. (p.26, ll.27-29).
<p>producing a negotiated control set resulting from said interaction between said first and second control sets.</p>	<p>Applicants disclose that the user program executes a transaction, whereby digital money is extracted from the buy order data package and transferred to the sell order package. Then the control data of the sell order data package is updated (i.e., producing a negotiated control set) after the matching of buy and sell orders (i.e., as a result of an interaction between the first control set and the second control set). (p.26, l.29-p.27, l.2).</p>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>131. A system for supporting electronic commerce including:</p>	<p>Applicants disclose an electronic system for supporting a broker-user business relationship (i.e., electronic commerce). (p.14, ll.26-29).</p>
<p>means for creating a first secure control set at a first location;</p>	<ul style="list-style-type: none"> Applicants disclose a data provider (e.g., an author) may secure control data with a data object on the data provider's data processor (i.e., first location) including a data packaging program (i.e., means for creating a first secure control set). (p.11, l.21-p.12, l.22). <i>See also</i> Claims 130 above and 132 below.
<p>means for creating a second secure control set at a second location;</p>	<ul style="list-style-type: none"> Applicants disclose a broker may repackage a received data package and add further control data (i.e., a second secure control set) which is relevant to his business activities with a data packaging program on the broker's data processor (i.e., means at a second location). (p.8, ll.9-16; p.8, l.25-p.10, l.14). <i>See also</i> Claims 130 above and 132 below.
<p>means for securely communicating said first secure control set from said first location to said second location; and</p>	<ul style="list-style-type: none"> Applicants disclose an author may provide a data object in a secure package from the author's data processor (i.e., first location) including network and telecommunications programs (i.e., means for communicating) to a broker's data processor (i.e., second location). (p.8, ll.9-16; p.8, l.25-p.9, l.9). <i>See also</i> Claims 130 above and 132 below.

means at said second location for securely integrating said first and second control sets to produce at least a third control set comprising plural elements together comprising an electronic value chain extended agreement.

- Applicants disclose a broker may create a parent composite object with control elements referring to constituent objects (i.e., first and second control sets) and the parent object (i.e., a third control set). (p.24, ll.11-26; FIG. 17).
- *See also* Claims 130 above and 132 below.

<p align="center">Copied Claim From InterTrust Published Patent Application</p> <p align="center">(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p align="center">Applicants' Disclosure in Appl. No. 09/321,386</p> <p align="center">(MDNA1.C2.US) (M-15081US)</p>
<p>132. A system for supporting electronic commerce including:</p>	<p><i>See Claim 131 above.</i></p>
<p>means for creating a first secure control set at a first location;</p>	<p>Applicants disclose a buyer that creates control data, e.g. kind of stock, price, quantity (i.e., a first secure control set) on the buyer's data processor (i.e., a first location). (p.26).</p>
<p>means for creating a second secure control set at a second location;</p>	<p>Applicants disclose a seller that creates control data, e.g. kind of stock, price, quantity (i.e., a second secure control set) on the seller's data processor (i.e., a second location). (p.26).</p>
<p>means for securely communicating said first secure control set from said first location to said second location; and</p>	<ul style="list-style-type: none"> • Applicants disclose a buyer's control data being sent to a stock trading company (p.26). It is inherent that a buyer's control data could be sent to a seller's data processor or vice versa. • Also, Applicants disclose an author may provide a data object in a secure package from the author's data processor (i.e., first location) including network and telecommunications programs (i.e., means for communicating) to a broker's data processor (i.e., second location). (p.8, ll.9-16; p.8, l.25-p.9, l.9).
<p>negotiation means at said second location for negotiating an electronic contract through secure execution of at least a portion of said first and second secure control sets.</p>	<ul style="list-style-type: none"> • Applicants disclose performing automated negotiations at the data processor of the stock trading company. (p.27, ll.3-4). Upon identifying matched buy and sell orders, the user program executes a transaction. (p.26, ll.29-30). • Thus, it is at least inherent that negotiations can occur at the seller's data processor.

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>133. A secure component-based operating system including:</p>	<p>See Claim 117 above.</p>
<p>component retrieving means for retrieving at least one component;</p>	<ul style="list-style-type: none"> • See Claim 117(a) above. • Applicants disclose a file transfer program that can transfer and receive files via a network to and from other data processors. (p.18, ll.25-26; FIG.14).
<p>record retrieving means for retrieving a record that specifies a component assembly;</p>	<ul style="list-style-type: none"> • See Claim 117(b) above. • Applicants disclose a usage manager module that calls 1) a decryption module that decrypts and extracts control data from a data package and 2) a control data parser module to extract data fields from usage elements (i.e., record retrieving means). (p.19, ll.13-19; FIG.14).
<p>checking means, coupled to said component retrieving means and said record retrieving means, for checking said component and/or said record for validity;</p>	<ul style="list-style-type: none"> • See Claim 117(c) above. • Applicants disclose decryption modules and security modules (i.e., checking means) that apply access control and verification using encryption/key methods such as RSA. (p.17, ll.27-29; p.21, ll.17-31; FIG.14).
<p>using means, coupled to said checking means, for using said component to form said component assembly in accordance with said record; and</p>	<ul style="list-style-type: none"> • See Claim 117(d) above. • Applicants disclose a usage manager module that unpackages and enables data object usage. (p.19, ll.13-28; FIG.14).

performing means, coupled to said using means, for performing a process based at least in part on said component assembly.

- See Claim 117(e) above.
- Applicants disclose a user program (i.e., performing means) that controls the usage of a data object in accordance with the control data included in the data package together with the data object. (p.17, ll.15-16; FIG.14).

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>134. A secure component-based operating system including:</p>	<p><i>See Claims 117 and 133 above.</i></p>
<p>a database manager that retrieves, from a secure database, at least one component and at least one record that specifies a component assembly;</p>	<ul style="list-style-type: none"> • <i>See Claims 117(a) and 133 above.</i> • Applicants disclose a memory that can store a received data package and a database intended for control data. (p.17, ll.9-12).
<p>an authenticating manager that checks said component and/or said record for validity;</p>	<p><i>See Claims 117(c) and 133 above.</i></p>
<p>a channel manager that uses said component to form said component assembly in accordance with said record; and</p>	<p><i>See Claims 117(d) and 133 above.</i></p>
<p>an execution manager that performs a process based at least in part on said component assembly.</p>	<p><i>See Claims 117(e) and 133 above.</i></p>

Copied Claim From InterTrust Published Patent Application (Ginter et al., Pub. No. US 2002/0112171 A1)	Applicants' Disclosure in Appl. No. 09/321,386 (MDNA1.C2.US) (M-15081US)
135. A secure component operating system including:	<i>See Claims 117 and 133-134 above.</i>
means for receiving a component;	<i>See Claims 117(a) and 133-134 above.</i>
means for receiving directions specifying use of said component to form a component assembly;	<i>See Claims 117(b) and 133 above.</i>
means, coupled to said receiving means, for authenticating said received component and/or said directions;	<i>See Claims 117(c) and 133-134 above.</i>
means, coupled to said authenticating means, for forming, using said component, said component assembly based at least in part on said received directions; and	<i>See Claims 117(d) and 133-134 above.</i>
means, coupled to said forming means, for using said component assembly to perform at least one operation.	<i>See Claims 117(e) and 133-134 above.</i>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>136. A secure component operating environment including:</p>	<p><i>See Claims 117 and 133-135 above.</i></p>
<p>a storage device that stores a component and directions specifying use of said component to form a component assembly;</p>	<p><i>See Claims 117(a) and 133-135 above.</i></p>
<p>an authenticating manager that authenticates said component and/or said directions;</p>	<p><i>See Claims 117(c) and 133-135 above.</i></p>
<p>a channel manager that forms, using said component, said component assembly based at least in part on said directions; and</p>	<p><i>See Claims 117(d) and 133-135 above.</i></p>
<p>a channel that executes said component assembly to perform at least one operation.</p>	<p><i>See Claims 117(e) and 133-135 above.</i></p>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>137. A secure operating system environment comprising:</p>	<p><i>See Claims 117 and 133-136 above.</i></p>
<p>a storage device that stores code and directors specifying assembly of said code into an executable program;</p>	<p><i>See Claims 117(a) and 133-136 above.</i></p>
<p>a validating device that checks said received code and/or said assembly directors for validity; and</p>	<p><i>See Claims 117(c) and 133-136 above.</i></p>
<p>an event-driven channel that, in response to occurrence of an event, assembles said code in accordance with said assembly directions to form an assembly for execution.</p>	<p><i>See Claims 117(d), 119, and 133-136 above.</i></p>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>138. A secure operating environment system for managing at least one resource comprising:</p>	<ul style="list-style-type: none"> • See Claim 120 above. • Applicants disclose a secure data processor. See Claim 119 above.
<p>a communications arrangement that securely receives a first control from a first entity external to said operating environment, and securely receives a second control from a second entity external to said operating environment, said second entity being different from said first entity; and</p>	<ul style="list-style-type: none"> • See Claims 120 and 131-137 above. • Applicants disclose network and telecommunications programs between authors and brokers and between buyers, sellers, and stock trading companies.
<p>a protected processing environment, coupled to said communications arrangement, that:</p>	<ul style="list-style-type: none"> • See Claims 120 and 131-137 above. • Applicants disclose secure data processors.
<p>(a) securely processes, using at least one resource, a data item associated with said first and second controls, and</p>	<p>See Claims 120 and 131-137 above.</p>
<p>(b) securely applies said first and second controls to manage said resource for use of said data item.</p>	<p>See Claims 120 and 131-137 above.</p>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
139. A system for negotiating electronic contracts, comprising:	<i>See Claims 131-138 above.</i>
a storage arrangement that stores a first control set received from a remote site, and stores a second control set;	<i>See Claims 131-138 above.</i>
a protected processing environment, coupled to said storage arrangement, that:	<i>See Claims 131-138 above.</i>
(a) performs an electronic negotiation between said first control set and said second control set,	<i>See Claims 131-138 above.</i>
(b) provides interaction between said first and second control sets, and	<i>See Claims 131-138 above.</i>
(c) produces a negotiated control set resulting from said interaction between said first and second control sets.	<i>See Claims 131-138 above.</i>

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>140. A method for supporting electronic commerce including:</p>	<p><i>See Claims 130-132 above.</i></p>
<p>creating a first secure control set at a first location;</p>	<p><i>See Claims 130-132 above.</i></p>
<p>creating a second secure control set at a second location;</p>	<p><i>See Claims 130-132 above.</i></p>
<p>securely communicating said first secure control set from said first location to said second location; and</p>	<p><i>See Claims 130-132 above.</i></p>
<p>electronically negotiating, at said second location, an electronic contract, including the step of securely executing at least a portion of said first and second secure control sets.</p>	<p><i>See Claims 130-132 above.</i></p>

<p align="center">Copied Claim From InterTrust Published Patent Application</p> <p align="center">(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p align="center">Applicants' Disclosure in Appl. No. 09/321,386</p> <p align="center">(MDNA1.C2.US) (M-15081US)</p>
141. An electronic appliance comprising:	Applicants disclose an electronic appliance. (p.17, ll.1-12).
a processor; and	Applicants disclose a data processor with a CPU. (p.17, ll.2-3).
at least one memory device connected to said processor;	Applicants disclose memory connected to a processor. (p.17, ll.4-12; FIG.13).
wherein said processor includes:	
retrieving means for retrieving at least one component, and at least one record that specifies a component assembly, from said memory device,	See Claims 117(b) and 133-137 above.
checking means coupled to said retrieving means for checking said component and/or said record for validity, and	See Claims 117(c) and 133-137 above.
using means coupled to said retrieving means for using said component to form said component assembly in accordance with said record.	See Claims 117(d) and 133-137 above.

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
142. An electronic appliance comprising:	<i>See Claim 141 above.</i>
at least one processor;	<i>See Claim 141 above.</i>
at least one memory device connected to said processor; and	<i>See Claim 141 above.</i>
at least one input/output connection coupled to said processor,	Applicants disclose that a display, a keyboard, a printer, a sound system, a ROM, and a bulk storage device may be connected to a bus connected to the CPU. (p.17, ll.1-12).
wherein said processor at least in part executes a rights operating system to provide a secure operating environment within said electronic appliance.	Applicants disclose a user program that controls the usage of a data object (i.e., a rights operating system). The user program is executed by the user's secure data processor. (p.17, ll.15-16; p.19, ll.5-7).

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>143. A method for auditing the use of at least one resource with a secure operating environment, said method comprising:</p>	<p>Applicants disclose sending of audit-like information related to use of a resource.</p>
<p>securely receiving a first control from a first entity external to said operating environment;</p>	<p><i>See Claims 120 and 130-132 above.</i></p>
<p>securely receiving a second control from a second entity external to said operating environment, said second entity being different from said first entity;</p>	<p><i>See Claims 120 and 130-132 above.</i></p>
<p>using at least one resource;</p>	<p><i>See Claims 120 and 130-132 above.</i></p>

securely sending to said first entity in accordance with said first control, first audit information concerning use of said resource; and

- Applicants disclose that one level of security for a broker may be to require on-line confirmation when loading a data object to the user's data processor to permit the broker to check that the object has not already been loaded as well as to double check all other parameters (i.e., audit report). (p.23, 1.29-p.24, 1.2). Furthermore, Applicants disclose that security modules could require a dial up to the brokers data processor to approve loading or usage actions and to implement approval authentication mechanisms. (p.25, 11.11-13).
- Thus, it is at least inherent that audit information, like a usage request, could be sent to a broker/data object provider upon use of a data object.
- Applicants disclose that a copy of a user set of control data is preferably stored in the broker's control database to provide a record with which to compare subsequent use, e.g., when a dial-up is required for usage. Thus, it is inherent that either control data is equivalent to audit information or that a broker/agent provides a two-way conduit for rights and audit data between content creators and content users.
- Applicants also disclose that the control data of both buy and sell order packages are updated to provide an audit trail after the transaction and transferred back to their authors (i.e., sending of audit information concerning use). (pp.26-27).

securely sending to said second entity in accordance with said second control, second audit information concerning use of said resource, said second audit information being at least in part different from said first audit information.

Id. See above.

<p>Copied Claim From InterTrust Published Patent Application</p> <p>(Ginter et al., Pub. No. US 2002/0112171 A1)</p>	<p>Applicants' Disclosure in Appl. No. 09/321,386</p> <p>(MDNA1.C2.US) (M-15081US)</p>
<p>144. A method for auditing the use of at least one resource with a secure operating environment, said method comprising:</p>	<p><i>See Claims 120 and 143 above.</i></p>
<p>securely receiving first and second control alternatives from an entity external to said operating environment;</p>	<ul style="list-style-type: none"> • Applicants disclose receiving buy and sell order controls, which may not match, at a stock trading company's data processor. (p.26)
<p>selecting one of said first and second control alternatives;</p>	<ul style="list-style-type: none"> • Applicants disclose either matching or not matching buy and sell order controls, which is equivalent to selecting one of the control alternatives.
<p>using at least one resource;</p>	<p><i>See Claim 143 above.</i></p>
<p>if said first control alternative is selected by said selecting step, securely sending to said entity in accordance with said first control alternative, first audit information concerning use of said resource; and</p>	<p><i>See Claims 120 and 143 above.</i></p>
<p>if said second control alternative is selected by said selecting step, securely sending to said second entity in accordance with said second control alternative, second audit information concerning use of said resource, said second audit information being at least in part different from said first audit information.</p>	<p><i>See Claims 120 and 143 above.</i></p>

Pursuant to 37 C.F.R. §1.604(a)(1), Applicants propose at this time that each of the claims being copied be deemed a count for the purposes of provoking an interference. However, we reserve the right to alter the counts if necessary.

The present application was filed on May 27, 1999 as a continuation of U.S. Patent Application No. 09/164,606, filed on October 1, 1998, which in turn claimed priority to U.S. Patent Application No. 08/594,811, filed on January 31, 1996, now U.S. Patent No. 5,845,281, which in turn claimed priority to Swedish Application No. 9500355-4, filed on February 1, 1995. The present application is based on substantially the same disclosure as U.S. Patent Application No. 08/594,811, now U.S. Patent No. 5,845,281, which contained substantially the same disclosure as in Swedish Application No. 9500355-4. Thus, added claims 111-144 are supported by the disclosure of Swedish Application No. 9500355-4 and are entitled to a priority date of February 1, 1995.

The aforementioned added claims 111-116 are copied from U.S. Patent Application No. 09/948,806, Publication No. 2002/0048369, published on April 25, 2002 for Ginter et al. as a division of U.S. Patent Application No. 09/272,998, filed on March 19, 1999, which is a continuation of U.S. Patent Application No. 08/706,208, filed on August 30, 1996, now abandoned. Thus, because the present application has a priority date earlier than the priority date of Ginter Appl. '806, Applicants allege that based at least upon priority of invention, Applicants are entitled to a judgment relative to the inventors of Ginter Appl. '806.

35 U.S.C. § 135(b)(2) does not bar this amendment because the amendment is being filed within twelve months of the publication date of the target patent application, April 25, 2002.

The aforementioned added claims 117-144 are copied from U.S. Patent Application No. 09/764,370, Publication No. 2002/0112171, published on August 15, 2002 for Ginter et al. as a continuation of U.S. Patent Application No. 09/335,465, filed on June 17, 1999, now U.S. Patent No. 6,237,786, which is a continuation of U.S. Patent Application No. 08/780,393, filed on January 8, 1997, now U.S. Patent No. 5,915,019, which is a division of U.S. Patent Application No. 08/388,107, filed on February 13, 1995, now abandoned. Thus, because the present application has a priority date earlier than the priority date of Ginter Appl.

'370, Applicants allege that based at least upon priority of invention, Applicants are entitled to a judgment relative to the inventors of Ginter Appl. '370.

35 U.S.C. § 135(b)(2) does not bar this amendment because the amendment is being filed within twelve months of the publication date of the target patent application, August 15, 2002.

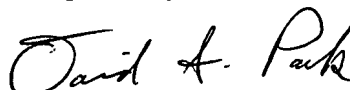
CONCLUSION

Accordingly, Applicants respectfully request that an interference be declared between the present Applicants and the inventors of the aforementioned patent applications. If there are any questions, please do not hesitate to call the undersigned at (949) 752-7040.

Express Mail Label No.:

EV 252 518 564US

Respectfully submitted,



David S. Park
Attorney for Applicants
Reg. No. 52,094